Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu

Malware : Reverse engineering

In this course, we address the issue of malware, a major societal concern. IT infrastructures now require security specialists to prevent attacks and analyze the damage caused by malware.
The lesson plan is in three parts :
– What is a malware: taxonomies and different types and capabilities of malware. Analysis of classic schemes of compromises and adjacent infrastructures.
– Malware analysis; Review of the basics needed for Windows process and assembly language operation. Triages techniques, dynamic and static analysis. Use of debugger, decompilers and disassembler. Using flow control graphs. Use of forensic detection tools.
– Technique used by malware; Obfuscations of code, function call and flow. Encryption, polymorphisms and variations, Stealth.

Détails

- Code : ISMS-MAL
- Durée : 3 jours (21 heures)

Public

- System administrators
- System architects and IT administrators
- Systems engineers

Pré-requis

Objectifs

Programme

What is a malware

- Taxonomies and different types and capabilities of malware
- Analysis of classic schemes of compromises and adjacent infrastructures

Malware analysis

- Review of the basics needed for Windows process and assembly language operation
- Triages techniques, dynamic and static analysis
- Use of debugger, decompilers and disassembler
- Using flow control graphs
- Use of forensic detection tools

Technique used by malware

- Obfuscations of code, function call and flow
- Encryption, polymorphisms and variations, Stealth

Modalités

- Type d'action :Acquisition des connaissances
- Moyens de la formation :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- Modalités pédagogiques :Exposés – Cas pratiques – Synthèse
- Validation :Exercices de validation – Attestation de stages